ABSTRACT OF THE DISCLOSURE

When generating a common key for use in an encryption process of encrypting a plaintext into a ciphertext and a decryption process of decrypting the ciphertext into the plaintext, components which are contained in the secret keys of one entity and correspond to other entity as a communicating party are extracted and composition of all the extracted components is performed while shifting the components to generate a common key. Thus, the common key consisting of a larger number of bits than the number of bits in each of the extracted components is generated. A common key of any size is generated by adjusting the amount of shift.